UNITED STATES DISTRICT COURT

DISTRICT OF VERMONT

IN THE MATTER OF THE SEARCH OF: 26 WATKINS ROAD MILTON, VERMONT	Case No. 2:18-MJ-135

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Caitlin Moynihan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 26 Watkins Road, Milton, Vermont, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B. As set forth below, I believe there is probable cause to believe that a computer device or devices located at the PREMISES has received, possessed, distributed, transported or accessed child pornography in violation of 18 U.S.C. § 2252A.

2. I am a Special Agent with Homeland Security Investigations (HSI). HSI is a directorate within Immigration and Customs Enforcement (ICE). ICE is a subordinate component of the Department of Homeland Security (DHS) and the successor to many of the law enforcement powers of the former Immigration and Naturalization Service and the former U.S. Customs Service. I have been a Special Agent since October 2009. I graduated from the Federal Law Enforcement Training Center in April 2010. I am currently assigned to the Burlington,

Vermont Residence Office. I hold a Bachelor of Arts degree in sociology from Providence College. I have participated in numerous child pornography investigations involving the use of peer-to-peer file sharing networks.

3. The statements in this affidavit are based on my personal observations, training and experience, investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are necessary to establish probable cause that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A are located at the PREMISES.

STATUTORY AUTHORITY

4. This investigation concerns alleged violations of Title 18, United States Code, § 2252A, and relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, distributing, receiving, reproducing for distribution, possessing or accessing with intent to view any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

PROBABLE CAUSE

CHARACTERISTICS OF CHILD PORNOGRAPHERS

5. Based upon my knowledge, experience, and training in child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to many individuals involved in such crimes:

a. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, or in some other secure location.

d. Likewise, those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area.

e. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with others to share information and materials.

BACKGROUND OF INVESTIGATION

6. Based upon my knowledge, experience, and training in child exploitation investigations, and the training and experience of other law enforcement officers with whom I have consulted, I know the following about peer-to-peer (P2P) file sharing:

a. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. To use P2P file sharing, a user must first obtain the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running the same or compatible P2P software. To obtain files on the network, a user opens the P2P software on the user's computer and conducts a search for files currently being shared on the network. The results of a search are displayed to the user. The user then selects file(s) from the results for download.

b. For example, a person interested in obtaining images of child pornography would open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects, from the results displayed, the file(s) he/she wants to download. The downloaded file is stored in the area previously designated by the user and/or the software. The downloaded file will remain until moved or deleted.

c. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file.

d. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address is unique to a particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.

e. The computer running the file sharing application has an IP address assigned to it while it is on the Internet. Computer users are able to see the IP address of computers sharing files on P2P networks.

7. Based on my training and experience, which includes experience investigating child exploitation cases, as well as my participation in a two-day training sponsored by the Internet Crimes Against Children task force on the use of the BitTorrent peer-to-peer network to facilitate investigations into users of the BitTorrent network, and the training and experience of the law enforcement personnel with whom I have spoken, I know the following about the BitTorrent file sharing network:

a. P2P file sharing networks, including BitTorrent, are frequently used to trade digital files of child pornography. These files include both still image and movie files.

b. To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used for the purpose of sharing digital files. Some examples are: uTorrent, Shareaza and BitLord.

c. It is the computers linked together through the Internet using this software that form the BitTorrent network that allows for the sharing of digital files between users. Most computers that are part of this network are referred to as "peers" or "clients."

d. During the installation of typical "BitTorrent" software, various settings are established which configure the host computer to share files. Depending upon the BitTorrent program used, a user may have the ability to

reconfigure some of those settings during installation or after the installation has been completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other BitTorrent users to download.

e. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network, a process referred to as "seeding."

f. To share a file or a set of files on the BitTorrent network, a "Torrent" file needs to be created by the user that initially wants to share a file or set of files. A Torrent is typically a small file that describes the file or files that are being shared, which may include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent program will have the ability to create a Torrent file. It is important to note that the Torrent file does not contain the actual file(s) being shared, but only information about the file(s) described in the Torrent, such as the name(s) of the file(s) being referenced in the Torrent and the "info hash" of the Torrent. The info hash is a SHA-1 hash value[1] of the set of data describing the file(s) referenced in the Torrent, which include the SHA-1 hash value of each file piece, the file size, and the file name(s). When another user (peer/client) later receives a particular piece, the hash of the piece is compared to the recorded hash to test that the piece is error-free.

g. Multiple persons sharing the same file(s) can deliver different pieces of the file(s) to the BitTorrent software on the downloading computer. BitTorrent software can only succeed in reassembling the pieces obtained from different users correctly if the individual pieces are exactly the same (digitally

[1] SHA1 hash values are obtained by applying a one-way mathematical algorithm to a digital file, of any length, to produce a fixed length output hash value. The resulting hash value is a unique and extremely compact alphanumeric representation of that file. Hash values are also known as digital signatures and are used in integrity protection and evidence verification in electronic discovery and computer forensics. It is computationally infeasible to find two different files which produced the same hash value when run through the above-referenced one-way mathematical algorithm.

identical). The BitTorrent program does this by matching the exact SHA-1 piece hash described in the Torrent file. Accordingly, the BitTorrent software can ensure that a complete and exact copy can be reconstructed from the parts.

h. Once a Torrent is created, in order to share the file(s) referenced in the Torrent file, a user typically makes the Torrent available to other users, such as via websites on the Internet.

i. For a typical user to locate Torrent files of interest and download the files that they describe, they use keyword searches on torrent indexing websites, historical examples of which include isohhunt.com and thepiratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate Torrent files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by Torrent files, only the Torrent file. Once a Torrent file is located on the website that meets a user's keyword search criteria, the user will download the Torrent file to their computer. The BitTorrent program on the user's computer will then process that Torrent file in order to find users (peers/clients) on the network that have all or part of the file(s) referenced in the Torrent file.

j. The actual file(s) referenced in the "Torrent" are obtained directly from other users (peers/clients) on the BitTorrent network. This means the download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the actual file(s) (not the torrent file but the actual files referenced in the .torrent file using any BitTorrent client.). Once completed, the downloaded file is then stored in the area previously designated by the user and/or the program. The downloaded file(s), including the torrent file, will remain until moved or deleted.

k. For example, a person interested in obtaining child pornography would open a torrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user selects a Torrent file from the results. This Torrent file represents the files the person wants to download. Once the Torrent file is downloaded, it is then used by a BitTorrent program which the user would have previously installed. The Torrent

file is the set of instructions the program needs to find the files referenced in the Torrent file. The files are then downloaded directly from the computer or computers sharing the file.

l. In the BitTorrent network, a "computer" could be a laptop or desktop computer, or it could also be a smart phone or tablet or other electronic device.

m. Even though the BitTorrent network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network without the receiving party's active participation. The software is designed only to allow files to be downloaded that have been selected for download by the receiver. It is impossible to send files from one computer to another without the receiver's permission or knowledge.

INFORMATION REGARDING SUBJECT PREMISES

8. On August 3, 2018, I was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. I identified a user with the IP address of 65.96.51.136 as a potential download candidate (source) of files of investigative interest. Files of investigative interest are files that have been previously identified by law enforcement officers as files of child exploitative materials based on their SHA values.

9. I directed my investigative focus to a device at IP address 65.96.51.136, because it was associated with a torrent with the infohash: 0ee3d720b358cc9d4d19ed5284be569ec74faf80. This torrent file references 109 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.

10. Using a computer running investigative BitTorrent software, I directly connected to the device at IP address 65.96.51.136. The user's BitTorrent software reported itself as: -UT340B - µTorrent 3.4.

11. On Friday, August 3, 2018, between 0144 hours and 0156 hours, I successfully completed the download of 15 files that the device at IP address 65.96.51.136 was making available; all of which I consider to be suspected child pornography.

a. The device at IP address 65.96.51.136 was the sole candidate for each download, and as such, each file was downloaded directly from IP address 65.96.51.136.

b. Two of the files are described as follows:

i. "(Luto) Peja_all (pedo gay pthc boy).wmv" This is a video file approximately 3 minutes and 25 seconds in length. This video depicts two male children approximately 6 to 10 years of age. The male children use their hands to stimulate each other's penises. At various points throughout the video, the male children perform oral sex on each other.

ii. "baby.wmv" This is a video file approximately 4 minutes and 52 seconds in length. This video depicts a nude prepubescent male child approximately 8 years old lying on his back, on what appears to be a bed. Another male, approximately 13 to 15 years of age is seen inserting his penis into the prepubescent male child's anus; this continues throughout the video. Later in the video, another nude prepubescent male child is observed lying on the bed.

12. On or about August 10, 2018, I searched publicly available records located online and determined that 65.96.51.136 was assigned to a company known as Comcast Cable Communications, LLC.

13. On August 28, 2018, the below information was received from Comcast regarding the subscriber of IP address 65.96.51.136 at the above date and times, as:

Subscriber Name:	Danny Weston
Service Address:	26 Watkins Rd, Milton, VT 05468
Subscriber Phone:	802-891-6629
Type of Service:	High Speed Internet Service
Account Number:	8773500030080565
Start of Service:	Unknown
Account Status:	Active
IP Assignment:	Dynamically Assigned
IP History:	See attached to date of Subpoena
E-mail User Ids:	dweston26@comcast.net, 61178590@comcast.net

14. In the days following receipt of that information, I conducted research into the subscriber, Danny Weston. I determined that Danny Weston had a year of birth of 1966 and a possible last known address of: 26 Watkins Road, Milton, Vermont. Record checks revealed that Danny Weston did not have any vehicles registered to him; he has a non-driver ID only. I received a photograph of Danny Weston from the Vermont Department of Motor Vehicles. Record checks conducted in the FBI Interstate Identification Index (III) and the State of Vermont criminal history databases for Danny Weston had negative responses.

15. On August 30, 2018, I received information from the Department of Labor. The response provided wage information for Danny Weston. The information indicated that as of quarter two in 2018, Weston was employed by: R L Vallee, Inc.

a. I conducted a search on Facebook for "Danny Weston" and located a page in which the male depicted in the profile picture appears to match the photograph provided by the DMV of Danny Weston.

b. Parts of this page are public and able to be viewed. The page lists "Maplefields At Chimney Corners" under the "work and education" section. Research indicated that R.L. Vallee operated convenience stores under the name Maplefields.

16. On September 4, 2018, SA Mike McCullagh and I conducted surveillance of the PREMISES. At approximately 0555 hours, no lights were observed on inside of the residence. A black Nissan sedan and a white Buick sedan were observed in the driveway; license plate numbers were not able to be obtained.

17. On September 5, 2018, SA McCullagh and I conducted surveillance of the PREMISES. At approximately 0610 hours, no lights were observed on inside of the residence. The black Nissan sedan and the white Buick sedan observed on the previous day were present again. There was also a motorcycle observed; no license plates were able to be obtained.

18. On September 10, 2018, SA McCullagh and I conducted surveillance of the PREMISES. At approximately 0545 hours, a vehicle was observed in the driveway with the lights on. SA McCullagh and I followed the vehicle once it departed the residence. The vehicle license plate was: HGR967. The vehicle was followed to Williston Road in South Burlington, at which time I observed the driver to be a female. Surveillance of that vehicle was discontinued at this time. Research conducted later indicated that the vehicle was registered to: Kaylyn Grenier at 26 Watkins Road in Milton, Vermont.

a. At approximately 0707 hours, SA McCullagh and I traveled to Maplefields located at 77 US-7 in Colchester, Vermont. I observed a male matching the photograph of Danny Weston working inside the store at this time.

19. On September 10, 2018, I checked with the United States Postal Service (USPS) to ascertain who was currently receiving mail at 26 Watkins Road in Milton, VT. A response was received on September 10, 2018, which indicated that the following names were receiving mail at that address: Brendan Sullivan and Patrick Grenier Sr.

20. I recognized the name of Brendan Sullivan and the address of 26 Watkin Road in Milton, Vermont. Further research indicated that HSI RAC Burlington assisted the Vermont Internet Crimes Against Children (ICAC) with an investigation in April 2018 in which Brendan Sullivan was arrested for violations of 13 V.S.A. § 2824 – Promoting a Recording of Sexual Conduct of a Child and 13 V.S.A. § 2827 – Possession of Child Pornography. Those charges are currently pending in state court. I assisted in the interview of Brendan Sullivan on April 18, 2018 and was present for the arrest of Sullivan.

21. On September 10, 2018, I contacted the Department of Motor Vehicles (DMV) and asked for registered vehicles and drivers associated with the PREMISES. On September 10, 2018, I received a response from the DMV which indicated seven names associated with the address, to include: Danny Weston, Lorie Grenier, Patrick Grenier, Kaylyn Grenier, and Brendan Sullivan.

22. I sent a request to the Vermont Fusion Center for information on Brendan Sullivan. The Vermont Intelligence Center (also known as the Fusion Center) provides accurate and timely strategic intelligence products to assist agencies with criminal cases, which includes but is not limited to background intelligence on persons suspected of criminal activity, timelines, and link charts to assist in organizing a case. The Fusion Center response indicted that Brendan Sullivan,

born in 1996, had a possible last known address of 16 Dubois Drive in South Burlington, Vermont. The response indicated that Brendan Sullivan was not associated with any vehicles; he has a non-driver ID only. The response indicated that the address associated with Brendan Sullivan's non-driver ID was: 26 Watkins Road in Milton, Vermont.

a. I also received a DMV photograph of Brendan Sullivan. I recognized the male in the photograph to be the individual that I interviewed on April 18, 2018, with Detective Matt Raymond of the Vermont Attorney General's Office and ICAC.

b. Record checks revealed that Sullivan had active conditions of release and was investigated for possession of child pornography – case numbers: 18SB004238, 14ADC0194, 15C203863. Record checks also indicated that Sullivan is reported as being autistic and aggressive. Sullivan was charged with theft for stealing money from his parents' safe. Record checks conducted in the FBI Interstate Identification Index (III) indicated that Brendan Sullivan had a FBI record number of: W8M78AD5N. A check of the State of Vermont criminal history databases for Brendan Sullivan indicated that Sullivan had a Vermont State ID number of: VT359802 – Possession of Child Pornography, arrest on April 18, 2018. Record checks also determined that Brendan Sullivan had a New Jersey State ID number of: NJ601823G and a Pennsylvania State ID number of: PA44350394.

23. I conducted research into Patrick Grenier and determined that he had a year of birth of 1965 and possible last known addresses of: 26 Watkins Road in Milton, Vermont. A response received from the Fusion Center indicated that Grenier is an employee of the Howard

Mental Health Center. The response also indicated that Grenier had the following vehicles registered to him: a 2005 Dodge Truck, white in color with VT tag: BLM466; a 2000 Pontiac Firebird, black in color with VT tag: EEL221 and a 2014 Honda Motorcycle, red in color with VT tag: HA268. A DMV photograph was received of Patrick Grenier. Record checks conducted in the FBI Interstate Identification Index (III) and the State of Vermont criminal history databases for Patrick Grenier had negative responses.

24. I conducted research into Lorie Grenier and determined that she had a year of birth of 1965 and a possible last known address of 26 Watkins Road in Milton, Vermont. Record checks revealed that Lorie Grenier had the following vehicles registered to her: a 2000 Pontiac Firebird, black in color with VT tag: EEL 221; a 1993 Saab, green in color with VT tag: EYR367 and a 2012 Buick white in color with VT tag: HDH413. A DMV photograph was received of Lorie Grenier. Record checks conducted in the FBI Interstate Identification Index (III) and indicated that Lorie Grenier had a negative response. A check of the State of Vermont criminal history databases for Lorie Grenier indicated that Lorie Grenier had a Vermont State ID number of: VT249405.

25. I conducted research into Kaylyn Grenier and determined that she had a year of birth of 1994 and a possible last known address of 26 Watkins Road in Milton, Vermont. Record checks revealed that Kaylyn Grenier had the following vehicle registered to her: a 2010 Honda Accord, silver in color, bearing VT tag: GMX 499. A DMV photograph was received of Kaylyn Grenier. Record checks conducted in the FBI Interstate Identification Index (III) and the State of Vermont criminal history databases for Kaylyn Grenier had negative responses.

26. On September 11, 2018, SA McCullagh and I traveled to the PREMISES and took photographs of the PREMISES.

27. On September 11, 2018, at approximately 0632 hours, SA McCullagh and I conducted surveillance of the PREMISES. At this time, no lights were observed on inside the residence and the white Buick was the only vehicle observed in the driveway. At approximately 0700 hours, a white Buick bearing VT tag: HDH413 (registered to Lorie Grenier) was observed at Maplefields located at 77 US-7 in Colchester, Vermont. Danny Weston was observed exiting the backseat of the vehicle and entered Maplefields. SA McCullagh and I followed the vehicle once it left Maplefields. The vehicle was occupied by a female driver and a male passenger. The male passenger resembled Brendan Sullivan. The vehicle returned to 26 Watkins Road in Milton, Vermont.

28. I have viewed the PREMISES and describe it here and in Attachment A as follows: a single family, one floor modular home, light gray in color with green shutters and a green door. It has a metal roof. The number 26 is displayed in black to the right of the front door.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP

address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses. There are two commonly used types of IP addresses called IPv4 and IPv6. IPv4, or IP version 4, is a 32-bit numeric address that consists of a series of four numbers, each ranging between 0 and 255, that are separated by dots. An example of an IPv4 address is 123.111.123.111. IPv6, or IP version 6, is a 128-bit hexadecimal address that consists of a series of eight values separated by colons. Hexadecimal values consist of a series of numbers between 0 and 9 and letters between A and F. An example of an IPv6 address is: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

d. "Child Pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

e. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

f. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

g. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have spoken, I know the following about computers and computer technology:

i. Computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed. Basically, computers serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

ii. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

iii. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store many thousands of images at very high resolution.

iv. The Internet affords individuals several different venues for meeting each other, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Individuals also use online resources to retrieve and store child pornography such as email services and cloud storage. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child

pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information

stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in

advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to view or share child pornography the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

33. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge

that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

35. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

36. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Caitlin Moynihan
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on October 1, 2018,

Hon. John M. Conroy
UNITED STATES MAGISTRATE JUDGE